Attorney's Docket No.: Intel 10559-225001 / P8790

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant :	Ernie F. Brickell et al.	Art Unit :	3621
Serial No.:	09/608,402	Examiner :	Daniel Greene
Filed :	June 30, 2000	Assignee :	Intel Corporation

Title: DIGITAL CREDENTIAL USAGE REPORTING

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

BRIEF ON APPEAL

Sir:

Since the claims, in their present form, have been twice rejected in the Office actions mailed June 1, 2004 and October 28, 2004, the application is ripe for appeal under 35 U.S.C. § 134(a). Accordingly, Appellant files this Brief on Appeal to perfect the Notice of Appeal filed herewith.

(1) Real Party in Interest

This case is assigned of record to Intel Corporation, who is hence the real party in interest.

CERTIFICATE OF MAILING BY FIRST CLASS MAIL

I hereby certify under 37 CFR §1.8(a) that this correspondence is being deposited with the United States Postal Service as first class mail with sufficient postage on the date indicated below and is addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

January 28, 2005
Date of Deposit

Signature

Carroll Allman
Typed or Printed Name of Person Signing Certificate

(2) Related Appeals and Interferences

There are no known related appeals and/or interferences.

(3) Status of Claims

Claims 1-56 are pending. Claims 1-56 stand rejected.

(4) Status of Amendments

No claim amendments have been filed.

(5) Summary of Claimed Subject Matter

The claims relate to storing and/or reporting the usage of digital credentials.

A user's "digital credential" is a security mechanism associated with a user's identity. *See* specification, page 2, line 16-17. Digital credentials thus identify the individual "owner" of the digital credential, rather than an account held by the owner. *Id.*, page 5, line 13-14. One example of a digital credential is a digital signature that can be attached to a message by the sender of the message. Such a digital signature allows the receiver to confirm that the message truly originated with a particular sender. *Id.*, page 1, line 8-23.

Digital credentials also have other uses. For example, digital credentials can be used by an owner to identify him- or

herself when accessing online services, presenting digitally signed documents, and conducting secure transactions. *Id.*, page 5, line 17-19. In one implementation, a digital credential can be used to identify a doctor who is submitting confidential medical diagnoses, prescription requests, or accessing confidential medical records. *Id.*, page 11, line 10-19. It is important to note that many such uses of digital credentials do not involve account transactions at all.

The applicants have realized that records regarding the usage of digital credentials can be stored and/or reported. *Id.*, page 8, line 23-24 and page 9, line 7-10. Such storage and/or reporting allows the owner of the digital credential to detect fraudulent misuse of the digital credential. *Id.*, page 7, line 9-12. Since misuse of a digital credential need not involve an account transaction, such misuse often went undiscovered before the development of the systems and techniques described in the present application.

One such system and technique is the subject of claim 1. Claim 1 relates to a method that includes receiving a request to verify a use of a digital credential by a user of a digital credential (as described, e.g., id., page 6, line 17-19), the digital credential being a digital security mechanism associated with a user's identity (as described, e.g., id., page 2, line

16-17), the use occurring at a first of a plurality of different services where the digital credential can be used (as described, e.g., id., page 5, line 17-18); verifying the use of the digital credential in response to receipt of the request to verify (as described, e.g., *id.*, page 6, line 20-22); sending a result of the verification to the first service (as described, e.g., *id.*, page 6, line 14-16); storing the result of the verification in an activity log in a central service that communicates with each of said plurality of different services (as described, e.g., *id.*, page 7, line 1-2); and allowing specified users to access said result (as described, e.g., *id.*, page 7, line 9-12).

Another such system and technique is the subject of claim 13. Claim 13 relates to a computer-readable medium having instructions (as described, e.g., *id.*, page 14, line 12-14) for causing a computer to receive a request to verify a use of a digital credential by a user of a digital credential (as described, e.g., *id.*, page 6, line 17-19) at any of a plurality of different services where the digital credential can be used (as described, e.g., *id.*, page 5, line 17-18), the digital credential being a digital security mechanism associated with a user's identity (as described, e.g., *id.*, page 2, line 16-17); verify the use of the digital credential in response to receipt of the request to verify from a first service of the plurality

of different services (as described, e.g., *id.*, page 6, line 20-22); send a result of the verification to the first service (as described, e.g., id., page 6, line 14-16); store a result of the verification in an activity log in a central service that communicates with each of said plurality of different services (as described, e.g., id., page 7, line 1-2); and allow specified users to access said result (as described, e.g., id., page 7, line 9-12).

Another such system and technique is the subject of claim 23. Claim 23 relates to a system that includes a server (as described, e.g., *id.*, page 12, line 7-10), an activity log (as described, e.g., *id.*, page 7, line 1-2), and a communication part (as described, e.g., *id.*, page 7, line 12-page 8, line 4).

The server is to receive requests to verify digital credentials by a user of a digital credential (as described, e.g., *id.*, page 6, line 17-19) at any of a plurality of different services where the digital credential can be used (as described, e.g., *id.*, page 5, line 17-18), to verify the use of the digital credential in response to receipt of requests (as described, e.g., *id.*, page 6, line 20-22), and to send results from the verifications to the services (as described, e.g., id., page 6, line 14-16). The activity log is coupled to the server to store the results from the verifications in a central service

that communicates with each of said plurality of different services (as described, e.g., *id.*, page 7, line 1-2). The communication part is to allow specified users to access said results (as described, e.g., *id.*, page 7, line 12-page 8, line 4 and page 10, line 7-9).

Another such system and technique is the subject of claim 27. Claim 27 relates to an article that includes a computer-readable medium having data structures stored thereon (as described, e.g., *id.*, page 14, line 6-9). The data structures include a first data field to store a result from an verification of a digital credential by a user of a digital credential at any of a plurality of different services where the digital credential can be used (as described, e.g., *id.*, page 8, line 23-24), a plurality of data fields to store transaction information relating to each verification result in a central service that communicates with each of said plurality of different services (as described, e.g., *id.*, page 8, line 24 - page 9, line 6), and a data access structure, allowing specified users to access said results (as described, e.g., *id.*, page 7, line 18 - page 8, line 4 and page 10, line 7-9).

Another such system and technique is the subject of claim 30. Claim 30 relates to a method that includes receiving use information describing a first use of a digital credential by an

owner of a digital credential (as described, e.g., id., page 6, line 17-19), at any of a plurality of different services where the digital credential can be used (as described, e.g., id., page 5, line 17-18), the digital credential being a digital security mechanism associated with the owner's identity (as described, e.g., *id.*, page 2, line 16-17); receiving use information describing a second use of the digital credential by a delegate of the owner of the digital credential, at any of the plurality of different services where the digital credential can be used (as described, e.g., *id.*, page 6, line 17-19 in light of page 5, line 15-17); storing the use information in an activity log (as described, e.g., *id.*, page 7, line 1-2); generating an activity report for the delegate based on the activity log (as described, e.g., *id.*, page 7, line 18 - page 8, line 4); generating an activity report for the owner based on the activity log (as described, e.g., *id.*, page 7, line 18 - page 8, line 4); allowing said owner to view all reports (as described, e.g., *id.*, page 9, line 17-19); and allowing said delegate to view only the activity report for the delegate and not the activity report for the owner or activity reports for other delegates (as described, e.g., *id.*, page 9, line 19-21).

Another such system and technique is the subject of claim 42. Claim 42 relates to a method that includes storing use

information for a digital credential of a plurality of delegates who are delegated to use said digital credential by an owner (as described, e.g., *id.*, page 7, line 1-2 in light of page 5, line 15-17), the digital credential being a digital security mechanism associated with the owner's identity (as described, e.g., *id.*, page 2, line 16-17); processing the use information for each of said plurality of delegates to detect misuse (as described, e.g., *id.*, page 8, line 5-9 and page 9, line 22 - page 10, line 7); and generating an alert to the owner based on the detection of misuse (as described, e.g., *id.*, page 10, line 7-9).

Another such system and technique is the subject of claim 48. Claim 48 relates to a method that includes receiving transaction requests from a plurality of delegate users who are delegated from an owner, (as described, e.g., *id.*, page 4, line 5-10) wherein the transaction requests include digital credentials for the delegate users (as described, e.g., *id.*, page 4, line 5-10), the digital credentials being digital security mechanisms associated with users' identities (as described, e.g., *id.*, page 2, line 16-17); processing the transaction requests (as described, e.g., *id.*, page 3, line 21-23); and communicating transaction information to a central service, wherein the transaction information includes the

digital credentials of the delegates (as described, e.g., *id.*, page 8, line 20-22), the transaction information communicated to create, for the plurality of delegate users, activity reports regarding the usage of the digital credentials (as described, e.g., *id.*, page 7, line 18 - page 8, line 4), the activity reports created at the central service that said owner is allowed to view (as described, e.g., *id.*, page 9, line 17-19) while each delegate is allowed to view only their own activity report and not allowed to view reports for other delegates (as described, e.g., *id.*, page 9, line 19-21).

Another such system and technique is the subject of claim 53. Claim 53 relates to a method that includes receiving a request from a medical professional to access medical information at a remote service (as described, e.g., *id.*, page 11, line 10-13), wherein the request includes a digital credential for the medical professional (as described, e.g., *id.*, page 11, line 15), the digital credential being a digital security mechanism associated with the medical professional's identity (as described, e.g., *id.*, page 2, line 16-17); communicating transaction information describing the access request and the digital credential to a credential verification service (as described, e.g., *id.*, page 11, line 13-16); receiving a verification result from the credential verification

service (as described, e.g., *id.*, page 11, line 16-17); providing the medical professional access to the medical information based on the verification result (as described, e.g., *id.*, page 11, line 18-19); and receiving an activity report from the credential verification service (as described, e.g., *id.*, page 11, line 19-21), wherein the activity report lists the transaction information, the digital credential and the transaction result (as described, e.g., *id.*, page 11, line 22 - page 12, line 6).

(6) Grounds of Rejection

Independent claims 1, 13, and 23 stand rejected under 35 U.S.C. § 103(a) as obvious over U.S. Patent No. 6,021,202 to Anderson et al. (hereinafter "Anderson") and U.S. Patent No. 6,442,526 to Vance et al. (hereinafter "Vance"). The rejections of claims 1, 13, and 23 are based on the contention that account information is a digital credential associated with a user's identity. On the basis of this equivalence, the rejection also contends that the application of Anderson's and Vance's account information verification systems to the verification of digital credentials is obvious.

Although the rejection of claims 1 and 13 only relies on Anderson and Vance, the Office action mailed October 28, 2004

repeatedly refers to an application of U.S. Patent No. 6,105,010 to Musgrave (hereinafter "Musgrave") in rejecting claims 1 and 13. *See* page 17, boldfaced header, page 18, boldfaced header, page 19, top boldfaced header, and page 20, boldfaced header. For purposes of this summary of the grounds for rejection, Applicant has assumed that these references are typographical errors. However, for the sake of completeness, Applicant has discussed the relevance of Musgrave to the patentability of claim 1 and 13 in the arguments below.

Independent claim 27 was rejected under 35 U.S.C. § 103(a) as obvious over Anderson and Vance. The rejection of claim 27 is based on the contention that a data field to store an account transaction is a data field to store a result from a verification of a digital credential associated with a user's identity. On the basis of this equivalence, the rejection also contends that the application of Anderson's and Vance's account information verification systems to the verification of digital credentials is obvious.

Independent claim 30 was rejected under 35 U.S.C. § 103(a) as obvious over Anderson and Vance. The rejection of claim 30 is based on the contention that account information is a digital credential associated with a user's identity. On the basis of this equivalence, the rejection also contends that the

application of Anderson's and Vance's account information verification systems to the verification of digital credentials is obvious.

Claim 30 was also rejected under 35 U.S.C. § 101 as being directed to "non-statutory subject matter." However, the rejection explicitly acknowledges that claim 30 is within the statutory definition of subject matter in 35 U.S.C. § 101 (i.e., "In claim 1, the applicant claims a method...").

The rejection also appears to contend that the subject matter of claim 30 falls within an exception to 35 U.S.C. § 101 created by *In re Musgrave*, 431 F.2d 882 (CCPA 1970). In particular, the rejection contends that the method of claim 30 is performable "without the aid of any technology," "not within the technological arts," and therefore not patentable. The rejection also implies that claim 30 is not directed to producing concrete, tangible, and useful results, and therefore not patentable.

Although the rejection of claims 1 and 13 only relies on Anderson and Vance, the Office action mailed October 28, 2004 repeatedly refers to an application of Musgrave in rejecting claim 30. *See* page 19, lower boldfaced header and page 21, boldfaced header. For purposes of this summary of the grounds for rejection, Applicant has assumed that these references are

typographical errors. However, for the sake of completeness, Applicant has discussed the relevance of Musgrave to the patentability of claim 30 in the arguments below.

Independent claim 42 was rejected under 35 U.S.C. § 103(a) as obvious over Goldsmith. The rejection of claim 42 is based on the contention that account information is a digital credential associated with a user's identity. In particular, the rejection contends that the identification of data as a digital credential associated with a user's identity (rather than as account information) is a "nonfunctional" and "descriptive" distinction and hence irrelevant to patentability. Based on the equivalence of account information and digital credentials, the rejection also contends that the application of Goldsmith's account information verification system to the verification of digital credentials is obvious.

Independent claim 48 was rejected under 35 U.S.C. § 103(a) as obvious over Goldsmith and Vance. The rejection of claim 48 is based on the contention that account information is a digital credential associated with a user's identity. On the basis of this equivalence, the rejection also contends that the application of Anderson's and Vance's account information verification systems to the verification of digital credentials is obvious.

Independent claim 53 was rejected under 35 U.S.C. § 103(a) as obvious over Anderson and Goldsmith. The rejection of claim 53 is based on the contention that account information is a digital credential associated with a user's identity. On the basis of this equivalence, the rejection also contends that the application of Anderson's and Vance's account information verification systems to the verification of digital credentials is obvious.

(7) Argument

As discussed above, a common thread to the rejections is the assertion in the rejection that that account information is a digital credential associated with a user's identity.[1]

The rejections rely upon the alleged common knowledge and various references relating to conducting business with a credit card. The rejection has argued that the claims can be "paraphrased to a transaction utilizing a credit card." *See* page 3 of the Office action mailed October 28, 2004. Given the broad relevance of this issue to the claims, it is now addressed

[1] When the distinction between account information and digital credentials was identified to the Patent Office in the response filed January 8, 2004, the Patent Office acknowledged that none of the cited art involved digital credentials associated with a user's identity. *See* Office action mailed Feb. 5, 2004, page 2. The present Office action mailed October 28, 2004 abandons this acknowledgement and instead reasserts the former position (i.e., that account information is a digital credential associated with a user's identity).

before additional grounds for the patentability of the individual claims are discussed.

Initially, any notion that claims can be "paraphrased" for purposes of examination is respectfully traversed. Most specifically, however, Applicant submits that account information is not a digital credential associated with a user's identity and that the usage of a credit card does not involve the storage and/or recording of a verification of a digital credential. Simply put, an account is not an individual, nor is an individual an account. Although the identity of an individual may be relevant to whether or not that individual can legally access an account, the mere identification of the account does not also identify the individual. Instead, information that identifies an account is distinct from information that identifies an individual.

There is also a very basic distinction between digital credentials and account information. Consider the standard procedure of conducting business with a credit card. When a merchant verifies the validity of a credit card, the merchant verifies the validity of account identification information. However, if a merchant chooses to verify the credit card user's identity, the merchant relies upon the user's name, signature, and/or likeness on a driver's license. None of these can be

considered digital, nor is their verification stored and/or reported.

If credit card account information were sufficient, in isolation, to verify the identity of a card user, then there would be no need for credit cards to bear the account holder's name, signature, and/or likeness. This illustrates how account information is not the same as identity, notwithstanding the Examiner's contention that they are equivalent.

Thus, one of ordinary skill would understand that the credit card transactions relied on by the rejection do not involve a digital security mechanism at all, much less the storage and/or reporting of the usage of a digital credential. Instead, records of credit card transactions simply identify when a particular account was accessed, based on the presentation of account information to a merchant.

The distinction between account information and identity information is particularly relevant in contexts such as online transactions, remote access to medical records, and other situations where the security mechanism associated with a user's identity is digital. In these contexts, a user's identity is "verified" using a digital credential that is subject to copying in ways that a signature or likeness is not. The harm that can be done by misuse of such a digital credential is expansive. In

particular, misuse of a digital credential can potentially extend beyond financial accounts and into realms such as access to medical records, the handling of prescriptions, and digital signatures on documents and contracts. By storing and/or reporting on the usage of digital credentials using the claimed systems and techniques, the fraud promulgated through such copying can be reduced.

Therefore account information and identity information are not equivalent. In addition, it is not obvious to handle a digital credential associated with a user's identity in the same manner as account information.

Attention is respectfully directed to the cited art to support this contention. For example, in Anderson, an electronic financial instrument includes a digital signature in addition to the traditional account information. See Anderson, col. 23, line 41-49.

Despite the fact that identity information and account information are found on the same instrument, Anderson handles them differently. In particular, after a transaction is performed on the basis of such an instrument, a Demand Deposit Account (DDA) statement is sent by the payer's bank to the payer. See Anderson, col. 24, line 38-42. The DDA statement reflects the debit to the account, presumably without mention of

the results of the verification of digital signature. The DDA statement and other record keeping and notifications appear to occur only at the account level, and there is no independent storage of the results of the verification of the digital signature in a central service, nor are specified users allowed to access the results of the verifications. Thus, digital credential information is not treated like account information in Anderson.

As another example, U.S. Patent No. 6,105,010 to Musgrave (hereinafter "Musgrave")[2] describes that digital credentials are handled separately from account information, and the verification of digital records is a discrete counterpart to the verification of account information in credit card and other financial transactions. In particular, after a credential verification message is transmitted by biometric verification processor 22, there is no disclosure that biometric verification processor 22 performs further activities. In other words, there is no description that biometric verification processor 22 stores a record of the result of the credential verification in a central service, nor does biometric verification processor 22 allow specified users to access the results of the

[2] Musgrave became of record in the Office action mailed Feb. 5, 2004 as showing the verification of a digital credential associated with a user's identity.

verifications. Rather, record keeping appears to occur only at the account level, just as described in Anderson and the other art of record.

This counterpart operation thus highlights that one of ordinary skill would treat transaction information differently than digital credentials. With the counterpart operation, the verification of digital credentials is discarded and only account access, to a single account, is recorded.

Such counterpart operation thus rebuts the contention that the application of account security/authorization processes to digital credentials would be obvious to one of ordinary skill. Musgrave clearly knew about both digital credentials and account security/authorization processes and yet, when Musgrave combined the two, he did so in a manner other than presently claimed. In particular, Musgrave describes that account transactions are to be recorded whereas digital credential verifications are to be discarded, just as in Anderson. Accordingly, there is no support for the contention that it would be obvious to apply account security/authorization processes to digital credentials since Musgrave and Anderson clearly demonstrate operations involving both that is outside the scope of applicant's claims.

Further, the Office bears the burden of showing that it would be obvious to handle a digital credential associated with

a user's identity in the same manner as account information. Applicant respectfully submits that the Office has not carried this burden. In particular, the current rejections merely provide conclusory statements that credit card accounts and the like are digital credentials associated with the user's identity. *See, e.g.,* Office action mailed October 28, 2004, page 7, paragraph 2. Given that the burden of proof on this issue lies on the Office, it is respectfully submitted that such conclusory statements are inadequate to maintain the rejections.

Further, the mere fact that the claims were within the capabilities of one of ordinary skill is not sufficient to establish a *prima facie* case of obviousness. "Rather, particular findings must be made as to the reason the skilled artisan, with no knowledge of the claimed invention, would have selected these components for combination *in the manner claimed.*" *In re Kotzab*, 217 F.3d 1365, 1371 (Fed. Cir. 2000) (emphasis added).

Independent Claims 1, 13, and 23

Turning to the individual rejections, independent claims 1, 13, and 23 were rejected under 35 U.S.C. § 103(a) as allegedly being obvious over Anderson and Vance.

The rejection of claims 1, 13, and 23 refers to Col. 6, line 42-54 of Anderson as allegedly describing the verification

of a digital credential associated with a user's identity, the sending of a result of such a verification, and the storage of such a result. Applicant respectfully disagrees and instead submits that Anderson further illustrates the distinction between digital credentials and account information.

The cited portion of Anderson describes the verification of both a check and a signature. *See* Anderson, col. 6, line 45-48. The check includes account information associated with a financial account, whereas the signature is a credential associated with the user's identity. As discussed above, account information is not a digital credential associated with a user's identity. Moreover, the signatures verified by Anderson are not digital. On these bases alone, Anderson fails to describe or suggest every step, operation, and component recited in claims 1, 13, and 23.

Nevertheless, Anderson's handling of the verification of the analog signature is relevant to determining the way that one of ordinary skill would handle the verification of digital credentials associated with a user's identity. Once Anderson's bank verifies the signature, the bank discards all record of the verification. The bank does not send the result of the verification to a service, nor does the bank (or any other party) store the result of the verification in an activity log.

Indeed, a contention otherwise is somewhat nonsensical, given that an analog signature is not subject to multiple uses at different services. Rather, each analog signature is a unique and independent operation.

Given that Anderson describes that the results of the verification of an analog credential are to be discarded once verification has occurred, Applicant submits that Anderson teaches away from claims 1, 13, and 23. Thus, any rejection under 35 U.S.C. § 103(a) that relies upon Anderson would have to overcome Anderson's express teachings as to how the results of the verification of analog credentials are to be treated when combined with traditional account transaction systems.

Vance does nothing to remedy these deficiencies of Anderson. In particular, Vance has nothing to do with digital credentials. However, Vance does provide further evidence of differences in the ways that different information is handled.

In Vance, a traveler or a travel agent enters an employee number that identifies the traveler. *See* Vance, col. 5, line 1-7. Vance's system uses the employee number to retrieve employee travel preferences and to designate travel arrangements to the employee. *See* Vance, col. 5, line 8-10 and line 30-47.

The employee number is not a digital credential since it is not a security mechanism at all. However, even if one were to

take the employee number to be a digital credential associated with the user's identity and the retrieval of employee travel preferences to be a "verification" of the employee number, the result of this "verification" is not sent anywhere, nor is the result of this "verification" stored. Rather, once an interaction session is closed, Vance's system discards any record of the retrieval of employee travel preferences and only stores the results of the interaction session. If no changes to travel plans are made during the interaction session, then no record of the retrieval of employee travel preferences remains.

Vance thus also provides further evidence of distinctions in the ways that different types of information are handled.

In summary, since elements and/or limitations from each of independent claims 1, 13, and 23 are neither described nor suggested by the cited art, it is respectfully submitted that a *prima facie* case of obviousness has not been established. Accordingly, it is respectfully submitted that claims 1, 13, and 23, and the claims dependent therefrom, are allowable.

Independent Claim 30

The 35 U.S.C. § 103(a) Rejection:

Independent claim 30 was rejected under 35 U.S.C. § 103(a) as obvious over Anderson and Vance. Claim 30 relates to a

method that includes receiving use information describing a first use of a digital credential by an owner of a digital credential at any of a plurality of different services where the digital credential can be used, receiving use information describing a second use of the digital credential by a delegate of the owner of the digital credential at any of the plurality of different services where the digital credential can be used, storing the use information in an activity log, generating an activity report for the delegate based on the activity log, generating an activity report for the owner based on the activity log, allowing the owner to view all reports, and allowing the delegate to view only the activity report for the delegate and not the activity report for the owner or activity reports for other delegates. The digital credential is a digital security mechanism associated with the owner's identity.

The rejection of claim 30 again refers to col. 6, lines 42-54 as relating to use of a digital credential associated with a user's identity. As discussed above, account information is not associated with a user's identity. Anderson's analog signature is not digital. On these bases alone, Anderson fails to describe or suggest every element recited in claim 30.

Once again, taking Anderson's signatures to be digital security mechanisms leads to nonsensical results. Analog

signatures are not subject to multiple uses at different services, but rather are unique and independent credentials. Further, the signatures presumably cannot be "used" by a delegate of the owner at different services. Short of fraud, it is unclear how a delegate would "use" someone else's signature. Further, the generation of an activity report for the delegate based on such a use would seem to imply that Anderson's banks could distinguish between the signatures used by the delegate and the signatures used by the owner, thereby frustrating the fraud.

Indeed, since Anderson's analog signatures are derived from the physical characteristics of a single individual, Applicant submits that Anderson also teaches away from any activity related to use of a credential by a delegate of the owner. In particular, unless the delegate were to evade the purpose of Anderson's system and copy the physical characteristics of the owner, then Anderson's signatures could not be used by a delegate at different services without frustrating the purpose behind Anderson's signature verification system. Thus, any rejection under 35 U.S.C. § 103(a) that relies upon Anderson would use have Anderson's express teachings as to how credentials associated with an owner's identity are to be

verified when combined with traditional account transaction systems.

Vance does nothing to remedy this deficiency of Anderson. Vance has nothing to do with digital credentials. However, even if one were to take Vance's employee number to be a digital credential and the retrieval of employee travel preferences to be a "verification" of the employee number, the result of the retrieval of employee travel preferences is not sent anywhere, nor is the result of the retrieval of employee travel preferences stored. Rather, once an interaction session is closed, Vance's system discards any record of the retrieval of employee travel preferences and only stores the results of the interaction session.

It is therefore respectfully submitted that the rejection does not establish a *prima facie* case of obviousness. Accordingly, it is respectfully submitted that claim 30, and the claims dependent therefrom, are allowable.

The 35 U.S.C. § 101 Rejection:

Claim 30 was also rejected under 35 U.S.C. § 101 as being directed to "non-statutory subject matter." However, the rejection explicitly acknowledges that claim 30 is within the statutory definition of subject matter in 35 U.S.C. § 101 (i.e., "In claim 1, the applicant claims a method...").

The rejection also appears to contend that the subject matter of claim 30 falls within an exception to 35 U.S.C. § 101 created by *In re Musgrave*, 431 F.2d 882 (CCPA 1970). In particular, the rejection contends that the method of claim 30 is performable "without the aid of any technology," "not within the technological arts," and therefore not patentable. The rejection also implies that claim 30 is not directed to producing concrete, tangible, and useful results, and therefore not patentable.

To begin with, *Musgrave* was decided in 1970. This is 10 years before the Supreme Court held statutory subject matter under 35 U.S.C. § 101 to "include anything under the sun that is made by man." *Diamond v. Chakrabarty*, 447 U.S. 303 (1980). *Chakrabarty* made it clear that anything except for laws of nature, physical phenomena, and abstract ideas are patentable. There are clearly man-made processes under the sun that can be performed without the aid of any technology. Therefore, any interpretation of *Musgrave* that would require that man-made patentable processes must be performed with the aid of technology has been overruled.[3]

---

[3] Further, assuming *arguendo* that a judicial exception to 35 U.S.C. § 101 was indeed created by *Musgrave* and has survived subsequent rulings, Applicant respectfully submits that the scope of that exception has been misinterpreted. In particular, the court's decision in *Musgrave* did not, in any way, equivocate "the technological arts" with "arts requiring the aid of

Accordingly, Applicant submits that the subject matter of claim 30 remains statutorily patentable subject matter.

The rejection also implies that claim 30 does not produce "a concrete, tangible and useful result." Applicant respectfully disagrees.

It is well-established that "a concrete, tangible and useful result" does not require a physical transformation. *See, e.g., AT&T Corp. v. Excel Communications, Inc.*, 172 F.3d 1352, 1358-59 (Fed. Cir. 1999). Rather, a determination of specific values can constitute patentable subject matter under 35 U.S.C. § 101. *See State Street Bank & Trust Co. v. Signature Financial Group*, 149 F.3d 1368, 1373 (Fed. Cir. 1998)(holding that the production of "a final share price momentarily fixed for

---

technology." Indeed, the exact opposite conclusion is apparent from *Musgrave*.

Musgrave's claims dealt with the manipulation and interpretation of seismograph signals. Id. at 893. The signals could be manipulated either mechanically or manually. Id. Prior to the hearing in the U.S. Court of Customs and Patent Appeals (CCPA), the Board of Appeals of the U.S. Patent Office (Board) had upheld a rejection of Musgrave's process claims based on the Examiner's contention that certain steps in the claimed processes could be carried out in the human mind and were thus directed to non-statutory subject matter. Id. at 892-93.

In overturning the Board's decision, the CCPA held that it "cannot agree with the board that these claims … are directed to non-statutory processes merely because some or all the steps therein can also be carried out in or with the aid of the human mind or because it may be necessary for one performing the processes to think. All that is necessary, in our view, to make a sequence of operational steps a statutory 'process' within 35 U.S.C. § 101 is that it be in the technological arts." Id. at 893 (emphasis added).

Thus, the CCPA clearly and definitively declared processes carried out entirely in the human mind to be "in the technological arts." This squarely contradicts the interpretation of *Musgrave* presented in the rejection, which contends that an invention must require "the aid of technology" to be "within the technological arts."

recording and reporting purposes and even accepted and relied upon by regulatory authorities and in subsequent trades" amounts to the production of a useful, concrete, and tangible result.)

In claim 30, not only are specific values determined (i.e., an activity report is generated), but use information is both received and stored and individuals are allowed to view activity reports. Accordingly, Applicant submits that the subject matter of claim 30 produces a concrete, tangible, and useful result and hence recites patentable subject matter.

Independent Claim 42

Independent claim 42 was rejected under 35 U.S.C. § 103(a) as obvious over U.S. Patent No. 6,064,990 to Goldsmith (hereinafter "Goldsmith").

Claim 42 deals with a method that includes storing use information for a digital credential of a plurality of delegates who are delegated to use the digital credential by an owner, processing the use information for each of the delegates to detect misuse, and generating an alert to the owner based on the detection of misuse. The digital credential is a digital security mechanism associated with the owner's identity.

The rejection admits that Goldsmith does not describe or suggest a single step recited in claim 42. Namely, the rejection admits that Goldsmith neither describes nor suggests

storing use information for a digital credential, processing the use information to detect misuse of the digital credential, and generating an alert based on the detection of misuse of the digital credential.

Goldsmith describes a system that electronically notifies an individual of *all* account activity. *See* Goldsmith, col. 3, line 9-11. The notified individual is to review the notifications to identify unauthorized activity. *See* Goldsmith, col. 2, line 15-16. Rather than relying on the scope and content of Goldsmith, the rejection contends that the applicant has not established[4]

1) that a digital credential distinguishes itself from account information;

2) that processing use information to detect digital credential misuse distinguishes itself from unprocessed notifications of account activity; and

3) that generating an alert based on the detection of misuse of a digital credential distinguishes itself from regular notifications of unprocessed account activity.

---

[4] More particularly, the Office action argues that Applicant has not "disclosed" the enumerated distinctions. Given that the rejection is made under 35 U.S.C. § 103(a), applicant has assumed that the Examiner was not, in fact, contending that there was any insufficiency with the scope of Applicant's disclosure. If this is in error, the Examiner is requested to issue a rejection enumerating the ground for the insufficiency.

As discussed above, one of ordinary skill considers credential information to be distinct from account information. The daily credit card transactions relied upon by the Examiner illustrate this distinction, as do the Anderson and Musgrave references. Even though Applicant is under no burden to establish this distinction, it has been established by the references of record. Given that the burden of proof to the contrary is on the Office, a *prima facie* case of obviousness cannot be established by relying on a bald conclusory statement to the contrary.

Further, the contentions that processing use information is somehow not inherently distinguished from not processing access information and that generating alerts based on the detection of misuse is not inherently distinguished from regular notifications of *all* account activity fly in the face of logic and have an Orwellian aura. When "processing" is not distinguished from "not processing," war becomes peace and love becomes hate. Indeed, since Goldberg regularly notifies individuals of *all* account activity, Goldberg can fairly be said to teach away from the method of claim 42, since any alert based on the detection of misuse would generally obviate the need to notify of *any use* whatsoever.

Applicant respectfully submits that a *prima facie* case of obviousness cannot be established independently of the scope and content of the prior art. Without *some* support for the listed contentions, the rejection amounts to hindsight-based reconstruction of the applicant's claims. The rejection thus neglects both the requirement that a suggestion to combine the references in the manner claimed must be *founded in the prior art*, and that requirement that the *entirety of the teachings of the art (e.g., the teachings of Musgrave and general credit card transactions) must be considered* when formulating a rejection.

It is therefore respectfully submitted that claim 42 is patentable over Goldsmith. Accordingly, it is respectfully submitted that claim 42 and the claims dependent therefrom are allowable.

Independent Claim 48

Independent claim 48 was rejected under 35 U.S.C. § 103(a) as obvious over Goldsmith and Vance.

Claim 48 relates to a method that includes receiving transaction requests from a plurality of delegate users who are delegated from an owner, processing the transaction requests, and communicating transaction information to a central service. The transaction information includes the digital credentials of

the delegates. The transaction information is communicated to create, for the plurality of delegate users, activity reports regarding the usage of the digital credentials.

In rejecting claim 48, the action contends that col. 2, line 55-60 of Goldsmith deals with transaction requests that include digital credentials.

Applicant respectfully disagrees. The cited portion of Goldsmith deals with secured passwords. Goldsmith expressly states that these passwords are associated with and allow an individual to access specific bank or investment accounts. See, e.g., col. 2, line 53 (providing *access to an account* over a transaction device 4) and col. 1, line 15-19 ("If the user provides the correct password, … financial transactions for those accounts to which the token permits access [is permitted]"). *See also* col. 2, line 5-8 ("The present invention provided a system for immediately notifying a user of *account activity with respect to one of the user's financial accounts.*") (emphasis added).

Since the passwords are associated with specific bank or investment accounts, Applicant respectfully submits that they are not digital security mechanisms associated with a user's identity. Rather are associated with an account and outside the scope of claim 48. As such, Goldsmith fails to describe or

suggest communicating transaction information including digital credentials to create activity reports regarding the usage of the digital credentials.

Vance does nothing to remedy these deficiencies of Anderson. In particular, Vance has nothing to do with digital credentials since his employee numbers employee numbers are not security mechanisms at all. However, Vance does provide further evidence of differences in the ways that different information is handled.

In particular, even if one were to take the employee number to be a digital credential associated with the user's identity, reports regarding the usage of the employee numbers are not allowed to be viewed by anyone. Rather, once an interaction session is closed, Vance's system discards any record of the retrieval of employee travel preferences and only stores the results of the interaction session. Vance thus also provides further evidence of distinctions in the ways that different types of information are handled.

As discussed above, it is respectfully submitted that account identification information is distinct from digital credentials associated with a user's identity. Handling both in the same way is not obvious, especially in light of express

teachings in the art of record that they are to be treated differently.

As a result of these distinctions, Goldsmith and Vance fail to describe or suggest storing or processing use information for a digital credential. Accordingly, it is respectfully submitted that claim 48 and the claims dependent therefrom are allowable.

Independent Claim 53

Independent claim 53 was rejected under 35 U.S.C. § 103(a) as obvious over Anderson and Goldsmith.

Claim 53 relates to a method that includes receiving a request from a medical professional to access medical information at a remote service, communicating transaction information describing the access request and the digital credential to a credential verification service, receiving a verification result from the credential verification service, providing the medical professional access to the medical information based on the verification result, and receiving an activity report from the credential verification service. The request includes a digital credential for the medical professional. The digital credential is a digital security mechanism associated with the medical professional's identity.

The activity report lists the transaction information, the digital credential and the transaction result.

The rejection admits that Anderson does not describe the receipt of activity reports as recited in claim 53. However, the rejection contends that Goldsmith remedies this deficiency in Anderson and describes receiving an activity report from a digital credential verification service that lists transaction information, the digital credential, and the transaction result.

Applicant respectfully disagrees. Goldsmith has nothing to do with credential information. As discussed above, one of ordinary skill would consider credential information to be distinct from account information. The daily credit card transactions relied upon by the Examiner illustrate this distinction, as does the Musgrave reference. Since Goldsmith's passwords are associated with specific bank or investment accounts, they are not digital credentials within the meaning of claim 53.

In addition, applicant respectfully submits that neither Anderson nor Goldsmith describes or suggests communicating transaction information describing the access request and the digital credential to a credential verification service and receiving a verification result from a credential verification service. As to Anderson, the rejection points to FIG. 26 as

allegedly showing the communication of information describing the digital credential to a credential verification service and the receipt of a verification result from a credential verification service.

However, FIG. 26 does not show a credential verification service at all. Rather, FIG. 26 only shows doctors using "secure authenticators" to digitally sign medical records. *See* Anderson, col. 39, line 21-24. FIG. 26 thus does not show the communication of information describing the digital credential to a credential verification service and the receipt of a verification result at all, which Anderson indicates is done by in a manner similar to that used for Anderson's digital checks. *See* Anderson, col. 40, line 3-11.

Anderson relies upon public key cryptographic signatures to verify digital signatures on digital checks. *See* Anderson, col. 27, line 30-39. In this system, the public keys used to verify digital signatures are public. They can be published in a public directory or furnished by the payee to multiple parties. *See* Anderson, col. 28, line 46-51. The verification of the digital signatures can thus be done by the payee him/herself, rather than a third party. *See* Anderson, col. 27, line 3-6 (verification of digital signatures done by anyone who "knows the signer's public key").

Thus, there is no need for the communication of information describing the digital credential to a credential verification service and the receipt of a verification result from a credential verification service in Anderson. Not surprisingly, no credential verification service is mentioned in Anderson.

Even if one were to consider Goldsmith's passwords to be digital credentials, Goldsmith fails to remedy this deficiency in Anderson. Since Goldsmith's passwords are verified only by the institution that houses the associated financial account, no information describing the digital credential to a credential verification service is ever communicated to a credential verification service and no verification result is ever received from a credential verification service. Rather, the verification is performed "in-house."

Further, given that Anderson's digital signatures can be verified by anyone with the public key, it is highly unlikely that one of ordinary skill would start communicating information describing a digital credential to a credential verification service and introduce activity reports that lists transaction information, the digital credential, and the transaction result into Anderson's system. Such steps would be wholly unnecessary and unduly redundant in Anderson's system.

Since neither Anderson nor Goldsmith describes or suggests a credential verification service at all, much less communicating transaction information describing the access request and the digital credential to a credential verification service, receiving a verification result from the credential verification service, and receiving an activity report from the credential verification service, it is respectfully submitted that a *prima facie* case of obviousness has not been established. Accordingly, it is respectfully submitted that claims 53, and the claims dependent therefrom, are allowable.

Applicant asks that all claims be allowed.

The brief fee is enclosed. Please apply any other charges or credits to Deposit Account No. 06-1050.

Respectfully submitted,

Date: January 28, 2005

Scott C. Harris
Reg. No. 30,020
Attorney for Intel Corporation
By John F. Conroy
Reg. No. 45,485

Fish & Richardson P.C.
USPTO Customer No. **20985**
12390 El Camino Real
San Diego, California 92130
Telephone: (858) 678-5070
Facsimile: (858) 678-5099

Appendix of Claims

Claim 1. (Previously Presented) A method comprising:

receiving a request to verify a use of a digital credential by a user of a digital credential, the digital credential being a digital security mechanism associated with a user's identity, the use occurring at a first of a plurality of different services where the digital credential can be used;

verifying the use of the digital credential in response to receipt of the request to verify;

sending a result of the verification to the first service;

storing the result of the verification in an activity log in a central service that communicates with each of said plurality of different services; and

allowing specified users to access said result.

Claim 2. (Original) The method of claim 1 further including storing transaction information in the activity log.

Claim 3. (Original) The method of claim 2, wherein the transaction information includes at least one of a message that was signed using a digital signature key of the digital credential, a value of a transaction, an online service, an

internet protocol (IP) address, a date of the transaction and a time of the transaction.

Claim 4. (Original) The method of claim 1 further including generating an activity report from the activity log, wherein the activity report lists the stored verification results.

Claim 5. (Original) The method of claim 4 further including associating a name to a digital signature key of the digital credential, wherein the activity report lists the name of the digital signature key.

Claim 6. (Original) The method of claim 4, wherein generating the activity report includes generating the activity report upon request by an owner of the digital credential.

Claim 7. (Original) The method of claim 4, wherein generating the activity report includes generating the activity report each time the digital credential is verified.

Claim 8. (Original) The method of claim 4, wherein generating the activity report includes generating a report periodically.

Claim 9. (Original) The method of claim 1 further including analyzing the activity log to detect misuse of the digital credential.

Claim 10. (Original) The method of claim 6, wherein generating the activity report includes listing activity for a plurality of digital signature keys associated with the owner.

Claim 11. (Original) The method of claim 1 further comprising:

authorizing one or more delegates to use a delegated digital credential to act on behalf of the owner of the digital credential for specified functions, wherein verifying the use of the digital credential includes determining whether the delegated digital credential was authorized for the specific use.

Claim 12. (Previously Presented) The method of claim 4, wherein generating an activity report includes generating activity reports of the delegates of the user and wherein said allowing comprises allowing said user to view all reports, but allowing each said delegate to view only their own activity report, and not allowing each said delegate to view reports for other delegates.

Claim 13. (Previously Presented) An article comprising a computer-readable medium having computer-executable instructions stored thereon for causing a computer to:

receive a request to verify a use of a digital credential by a user of a digital credential at any of a plurality of different services where the digital credential can be used, the digital credential being a digital security mechanism associated with a user's identity;

verify the use of the digital credential in response to receipt of the request to verify from a first service of the plurality of different services;

send a result of the verification to the first service;

store a result of the verification in an activity log in a central service that communicates with each of said plurality of different services; and

allow specified users to access said result.

Claim 14. (Original) The article of claim 13, wherein the computer-executable instructions cause the computer to store transaction information in activity log.

Claim 15. (Original) The article of claim 14, wherein the transaction information includes at least one of a message that was signed using a digital signature key of the digital

credential, a transaction value, an online service processing the transaction, an internet protocol (IP) address of a computing device originating the transaction, the date of the transaction and the time of the transaction.

Claim 16. (Original) The article of claim 13, wherein the computer-executable instructions cause the computer to generate an activity report from the activity log, wherein the activity report lists the stored verification results.

Claim 17. (Previously Presented) The article of claim 16, wherein the computer-executable instructions cause the computer to associate a name to a digital signature key of the digital credential, wherein the activity report lists the name of the digital signature key.

Claim 18. (Previously Presented) The article of claim 16, wherein the computer-executable instructions cause the computer to generate the activity report upon receiving a request by an owner of the digital credential and wherein said allowing comprises allowing said user to view all reports, but allowing each said delegate to view only their own activity report, and not allowing each said delegate to view reports for other delegates.

Claim 19. (Original) The article of claim 13, wherein the computer-executable instructions cause the computer to analyze the activity log to detect misuse of the digital credential.

Claim 20. (Original) The article of claim 17, wherein the computer-executable instructions cause the computer to list in the activity report activity for a plurality of digital signature keys associated with the owner according to the name of the digital signature key.

Claim 21. (Original) The article of claim 20, wherein the computer-executable instructions cause the computer to authorize one or more delegates to use a delegated digital credential to act on behalf of the owner of the digital credential for specified functions and determine whether the delegated digital credential was authorized for the specific use.

Claim 22. (Original) The article of claim 21, wherein the computer-executable instructions cause the computer to generate activity reports of the delegates.

Claim 23. (Previously Presented) A system comprising:

a server to receive requests to verify digital credentials by a user of a digital credential at any of a plurality of different services where the digital credential can be used, to

verify the use of the digital credential in response to receipt of requests, and to send results from the verifications to the services;

an activity log coupled to the server to store the results from the verifications in a central service that communicates with each of said plurality of different services; and

a communication part to allow specified users to access said results.

Claim 24. (Original) The system of claim 23, wherein the activity log is configured to store transaction information for each authentication result.

Claim 25. (Original) The system of claim 24, wherein the transaction information includes at least one of a digitally signed message, a date of the transaction, a value of the transaction, an online service requesting the authentication, an internet protocol (IP) address, a value of the transaction, and a time of the transaction.

Claim 26. (Previously Presented) The system of claim 23, and further comprising an owner database to store information of an owner of the digital credential and owner-approved delegates and wherein said communication element allows said owner to view

all reports, but allows each said delegate to view only their own report, and not reports for other delegates.

Claim 27. (Previously Presented) An article comprising a computer-readable medium having data structures stored thereon comprising:

a first data field to store a result from an verification of a digital credential by a user of a digital credential at any of a plurality of different services where the digital credential can be used;

a plurality of data fields to store transaction information relating to each verification result in a central service that communicates with each of said plurality of different services; and

a data access structure, allowing specified users to access said results.

Claim 28. (Original) The article of claim 27, wherein the plurality of data fields store at least one of a digitally signed message, a date of the transaction, a time of the transaction, a value of the transaction, an online service, an internet protocol (IP) address of a computing device originating the transaction, and goods or services involved in the transaction.

Claim 29. (Original) The article of claim 27, wherein the data structures further include a plurality of data fields to store owner and delegate information.

Claim 30. (Previously Presented) A method comprising:

receiving use information describing a first use of a digital credential by an owner of a digital credential, at any of a plurality of different services where the digital credential can be used, the digital credential being a digital security mechanism associated with a the owner's identity;

receiving use information describing a second use of the digital credential by a delegate of the owner of the digital credential, at any of the plurality of different services where the digital credential can be used;

storing the use information in an activity log;

generating an activity report for the delegate based on the activity log;

generating an activity report for the owner based on the activity log;

allowing said owner to view all reports; and

allowing said delegate to view only the activity report for the delegate and not the activity report for the owner or activity reports for other delegates.

Claim 31. (Original) The method of claim 30, wherein the use information includes transaction information.

Claim 32. (Original) The method of claim 30, wherein the use information includes verification information for the digital credential.

Claim 33. (Original) The method of claim 31, wherein the transaction information includes at least one of a message that was signed, a transaction value, an online service, an internet protocol (IP) address, a value of the transaction, a date of the transaction and a the time of the transaction.

Claim 34. (Original) The method of claim 30, wherein the digital credential includes a digital signature key, and further wherein generating the activity report includes associating a name to the digital signature key and listing the name of the digital signature key.

Claim 35. (Previously Presented) The method of claim 30, wherein generating the activity report for the owner includes generating the activity report upon request by an owner of the digital credential.

Claim 36. (Original) The method of claim 30, wherein generating the activity report includes generating the activity report each time the digital credential is verified.

Claim 37. (Original) The method of claim 30, wherein generating the activity report includes generating a report periodically.

Claim 38. (Original) The method of claim 30 further including analyzing the activity log to detect misuse of the digital credential.

Claim 39. (Previously Presented) The method of claim 35, wherein generating the activity report includes listing activity for a plurality of digital signature keys associated with the owner.

Claim 40. (Previously Presented) The method of claim 30 further comprising:

authorizing one or more delegates to use a delegated digital credential to act on behalf of the owner of the digital credential for specified functions, wherein verifying the use of the digital credential includes determining whether the delegated digital credential was authorized for the specific use.

Claim 41. (Previously Presented) The method of claim 30, wherein generating the activity report for the owner includes generating activity reports of the delegates of the owner.

Claim 42. (Previously Presented) A method comprising:

storing use information for a digital credential of a plurality of delegates who are delegated to use said digital credential by an owner, the digital credential being a digital security mechanism associated with the owner's identity;

processing the use information for each of said plurality of delegates to detect misuse; and

generating an alert to the owner based on the detection of misuse.

Claim 43. (Original) The method of claim 42, wherein generating an alert includes generating an activity report based on the use information.

Claim 44. (Original) The method of claim 42, wherein generating an alert includes alerting a credential service provider.

Claim 45. (Previously Presented) The method of claim 42, wherein the use information includes transaction information and wherein the method further comprises allowing said owner to view

all reports, but allowing each said delegate to view only their own activity report, and not allowing each said delegate to view reports for other delegates.

Claim 46. (Original) The method of claim 42, wherein the use information includes verification information for the digital credential.

Claim 47. (Original) The method of claim 45, wherein the transaction information includes at least one of a message that was signed, a transaction value, an online service, an internet protocol (IP) address, a value of the transaction, a date of the transaction and a the time of the transaction.

Claim 48. (Previously Presented) A method comprising:

receiving transaction requests from a plurality of delegate users who are delegated from an owner, wherein the transaction requests include digital credentials for the delegate users, the digital credentials being digital security mechanisms associated with users' identities;

processing the transaction requests; and

communicating transaction information to a central service, wherein the transaction information includes the digital credentials of the delegates, the transaction information

communicated to create, for the plurality of delegate users, activity reports regarding the usage of the digital credentials, the activity reports created at the central service that said owner is allowed to view while each delegate is allowed to view only their own activity report and not allowed to view reports for other delegates.

Claim 49. (Original) The method of claim 48, wherein processing the transaction requests includes communicating the digital credentials to the central service for verification.

Claim 50. (Previously Presented) The method of claim 48, wherein processing a requested transaction includes:

verifying the digital credential; and

communicating a result of the verification to the credential service.

Claim 51. (Original) The method of claim 48 further including receiving a activity report from the central service, wherein the activity report lists the transaction information for each digital credential.

Claim 52. (Original) The method of claim 48, wherein the transaction information includes at least one of a message that was signed, a transaction value, an online service, an internet

protocol (IP) address, a value of the transaction, a date of the transaction and a the time of the transaction.

Claim 53. (Previously Presented) A method comprising:

receiving a request from a medical professional to access medical information at a remote service, wherein the request includes a digital credential for the medical professional, the digital credential being a digital security mechanism associated with the medical professional's identity;

communicating transaction information describing the access request and the digital credential to a credential verification service;

receiving a verification result from the credential verification service;

providing the medical professional access to the medical information based on the verification result; and

receiving an activity report from the credential verification service, wherein the activity report lists the transaction information, the digital credential and the transaction result.

Claim 54. (Original) The method of claim 53, wherein the transaction information includes at least an access type, a date of the transaction and a time of the transaction.

Claim 55. (Original) The method of claim 53, further wherein the digital credential was provided by a credential issuing service and a credential service provider.

Claim 56. (Original) The method of claim 53, and further including:

receiving a request to access the activity report from an owner of the digital credential; and

providing the owner access to the activity report.